

DIN EN 419111-5

ICS 35.240.15

Einsprüche bis 2013-05-25

Entwurf

**Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von
Signaturen –
Signaturprüfanwendung –
Teil 5: Mögliche Erweiterungen;
Englische Fassung prEN 419111-5:2013**

Protection profiles for signature creation and verification application –
Signature verification application –
Part 5: Possible extensions;
English version prEN 419111-5:2013

Profils de protection pour application de création et de vérification de signature –
Application de vérification de signature –
Partie 5 : Extensions possibles;
Version anglaise prEN 419111-5:2013

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-03-25 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 30 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

E DIN 419111-5 ist Teil der fünfteiligen Europäischen Normenreihe E DIN EN 419111 (entsprechend prEN 419111). Diese Normenreihe enthält Schutzprofile, welche die Sicherheitserfordernisse für das Erzeugen und das Prüfen von Signaturen definieren. E DIN EN 419111-5 enthält Gruppen von Sicherheitsfunktionen, die zum Kern-Schutzprofil für die Anwendung zum Prüfen von Signaturen (SVA PP) hinzugefügt werden können. Die folgenden Gruppen stehen zur Verfügung: Prüfer-Gruppe (en: checker package), Zertifikat-Management-Gruppe (en: certificate management package) und Gruppe für explizites Managen der Sicherheitsstrategie (en: Explicit Security Policy Management package).

Gemäß den Kriterien des DIN für den Verzicht auf die Erstellung einer deutschen Sprachfassung wurde auf eine deutsche Fassung verzichtet; E DIN 419111-5 enthält somit den englischen Originaltext, ergänzt um eine deutsche Übersetzung der verwendeten Begriffe und Definitionen.

Im IT-Sicherheitsbereich sind Schutzprofile (en: protection profiles) Bestandteil des Zertifizierungsprozesses gemäß der „Common Criteria“, d. h., der Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie (en: Common Criteria for Information Technology Security Evaluation, CC). Es handelt sich um die Festlegung einer implementierungsunabhängigen Menge von Mindestsicherheitsanforderungen für IT-Produkte bei einer gegebenen Sicherheitslage. Auf Basis dieser Schutzprofile können IT-Produkte geprüft werden und bei positivem Ausgang ein Zertifikat erhalten.

Die Normenreihe E DIN EN 419111 (entsprechend prEN 419111) ist Bestandteil einer Familie von Schutzprofilen, die von CEN als Europäische Normen zur Entwicklung von gemeinsamen Rahmenbedingungen für elektronische Signaturen in Auftrag gegeben worden sind. Weiterer Bestandteil der gemeinsamen Rahmenbedingungen ist z. B. die Normenreihe E DIN EN 14169 „Schutzprofile für Sichere Signaturerstellungseinheiten“.

Die fünf Teile der Europäischen Normenreihe E DIN EN 419111 beinhalten:

- Eine Einführung in die Normenreihe (E DIN EN 419111-1);
- die Festlegung der grundlegenden Funktionen, die für eine Anwendung zum Erzeugen von Signaturen unabdingbar sind. Hierbei handelt es sich um ein Schutzprofil gemäß CC, welche lediglich die benötigten Kernfunktionen spezifiziert (E DIN EN 419111-2);
- mögliche Ergänzungen zu den Funktionen von E DIN EN 419111-2 (E DIN EN 419111-3);
- die Festlegung der grundlegenden Funktionen, die für eine Anwendung zum Prüfen von Unterschriften unabdingbar sind. Hierbei handelt es sich um ein Schutzprofil gemäß CC, welches lediglich die benötigten Kernfunktionen spezifiziert (E DIN EN 419111-4); sowie
- mögliche Ergänzungen zu den Funktionen von E DIN EN 419111-4 (E DIN EN 419111-5).

E DIN EN 419111-5:2013 wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird. Das deutsche Spiegelgremium ist der NA 043-01-17 AA „Karten und persönliche Identifikation“.

Nationaler Anhang NA (informativ)

Literaturhinweise

E DIN EN 419111-1:2013, *Schutzprofile für eine Anwendung zum Erzeugen und Prüfen von Signaturen* —
Teil 1: Einführung

— Leerseite —

English Version

Protection profiles for signature creation and verification
application - Signature verification application - Part 5: Possible
extensions

Profils de protection pour application de création et de
vérification de signature - Application de vérification de
signature - Partie 5 : Extensions possibles

Schutzprofile für eine Anwendung zum Erzeugen und
Prüfen von Signaturen –
Signaturprüfanwendung – Teil 5: Mögliche
Erweiterungen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 224.

If this draft becomes a European Standard, CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

1	Scope	6
2	Normative references	6
3	Terms and definitions	6
4	Symbols and abbreviations	6
5	Extended component definition	6
5.1	Definition of the Family FDP_SVR	6
6	Checker package	8
6.1	Scope	8
6.1.1	Introduction	8
6.2	Conformance	8
6.2.1	CC Conformance Claim	8
6.2.2	EAL Claim	8
6.3	Security problem definition	8
6.3.1	Assets	8
6.3.2	Threats	8
6.3.3	Organisational security policies	9
6.3.4	Assumptions	9
6.4	Security objectives	9
6.4.1	Security objectives for the TOE	9
6.4.2	Security objectives for the operational environment	9
6.4.3	Rationale for Security objectives	9
6.5	Security requirements	9
6.5.1	Introduction	9
6.5.2	Security functional requirements	9
6.5.3	SFR / Security objectives	11
6.5.4	SFR Dependencies	12
7	Time stamp attribute package	14
7.1	Scope	14
7.1.1	Introduction	14
7.1.2	TS attribute computation	14
7.1.3	TS attribute verification	14
7.2	Conformance	15
7.2.1	CC Conformance Claim	15
7.2.2	EAL Claim	15
7.3	Security problem definition	15
7.3.1	Assets	15
7.3.2	Threats	15
7.3.3	Organisational security policies	15
7.3.4	Assumptions	15
7.4	Security objectives	15
7.4.1	Security objectives for the TOE	15
7.4.2	Security objectives for the operational environment	15
7.4.3	Rationale for Security objectives	15
7.5	Security requirements	16
7.5.1	Introduction	16
7.5.2	Security functional requirements	16
7.5.3	SFR / Security objectives	18
7.5.4	SFR Dependencies	18

8	Complete validation data attribute package	18
8.1	Scope	18
8.1.1	Introduction	18
8.1.2	Complete validation attribute computation	19
8.1.3	Complete validation attribute verification	19
8.2	Conformance	19
8.2.1	CC Conformance Claim	19
8.2.2	EAL Claim	19
8.3	Security problem definition	19
8.3.1	Assets	19
8.3.2	Threats	19
8.3.3	Organisational security policies	20
8.3.4	Assumptions	20
8.4	Security objectives	20
8.4.1	Security objectives for the TOE	20
8.4.2	Security objectives for the operational environment	20
8.4.3	Rationale for Security objectives	20
8.5	Security requirements	20
8.5.1	Introduction	20
8.5.2	Security functional requirements	21
8.5.3	SFR / Security objectives	22
8.5.4	SFR Dependencies	23
9	Explicit Policy-based ES package	23
9.1	Scope	23
9.1.1	Introduction	23
	Bibliography	24
	Index	26

Figures

Figure 1 — FDP_SVR component levelling	7
Figure 2 — Time stamp attribute TOE environment	14
Figure 3 — Complete validation data attribute TOE environment	19

Tables

Table 1 — Checker SFP – subjects, objects and attributes	9
Table 2 — Checker operation rules.....	10
Table 3 — security objective rationale - with Checker.....	11
Table 4 — SFR Dependencies	12
Table 5 — Time stamp - security objective rationale	15
Table 6 — Time stamp - object security attributes.....	16
Table 7 — Time stamp - attributes conditions and modifications	16
Table 8 — Time stamp - SFR/objectives rationale.....	18
Table 9 — Time stamp - SFR dependencies rationale	18
Table 10 — Complete validation data - security objective rationale	20
Table 11 — Complete validation data - object security attributes	20
Table 12.....	20
Table 13 — Complete validation data - attributes conditions and modifications	21
Table 14 — Complete Validation Data - SFR/objectives rationale	23
Table 15 — Complete Validation Data - SFR dependencies rationale.....	23

Foreword

This document (prEN 419111-5:2013) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

This document will supersede CEN/CWA 14171:2004.

EN 419111 consists of the following parts under the general title "*Protection profiles for signature creation and verification application*":

- *Part 1: Introduction.*
This part is an introduction to EN 419111;
- *Part 2: Signature creation application – Core PP.*
This part is a PP for the SCA, specifying only the core security functions;
- *Part 3: Signature creation application – Possible extensions.*
This part specifies possible additional security functions that can be added to the core SCA PP;
- *Part 4: Signature verification application – Core PP.*
This part is a PP for the SVA, specifying only the core security functions;
- *Part 5: Signature verification application – Possible extensions.*
This part specifies possible additional security functions that can be added to the core SVA PP.